UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/628,692	07/28/2000	W. Olin Sibert	7451.0025-00	3388

22852 7590 01/14/2004

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	8

DATE MAILED: 01/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/628,692	SIBERT, W. OLIN	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07/28/2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4,5,7* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Pursuant to USC 131, claims 1-27 are presented for examination.

1.1 The information disclosure statement filed 3/21/2003 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because in referring to paper No. 7, pages 13-21, the non-patent literatures are not initialed by the examiner for not being found in the enclosed application. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609 ¶ C(1).

Specification

2. The disclosure is objected to because of the following informalities: on page 19, line 8, reference number "106" should be --118--. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3.1 **Claims 7, 10-11, 13, and 27** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,047,242 to **Benson**.

3.2 **As per claim 7, Benson** discloses a computer system including an insecure computing arrangement for using an application, a trusted element for verifying the application comprising: a decryptor that decrypts a credential associated with the application (see column 12, lines 63-65); a validator that validates at least one digital signature corresponding to the credential (see column 11, lines 42-51); a challenge generator that selects, based at least in part on the credential, at least one predetermined portion of the application, and issues a challenge requesting a response providing a computation of at least one value based on the selected predetermined portion of the application (see columns 11-12); and a response checker that checks the response against the credential (see column 12, lines 50-54).

As per claims 10-11, Benson discloses the limitation of wherein the challenge generator requests the application to compute a cryptographic hash of the selected predetermined portion (see column 13).

As per claim 13, Benson discloses the limitation of wherein the challenge generator selects a virtual path within the application (see column 9, lines 40-45).

As per claim 27, Benson discloses a method for tampering with a credential verification process, the method including: predicting portions of a credentialed electronic item specified in repetitive challenges (see column 8 and column 9, lines 25-35), and supplying corresponding cryptographic hash values based on the predicted portions (see columns 8 and 13).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 1-6, 8, 9, 12, 14-26** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,047,242 to **Benson** in view of US Patent 6,009,543 to **Shavit**.

4.2 **As per claims 1 and 2, Benson** substantially teaches a method for verifying an electronic item, the method including: (a) presenting a secure credential, the credential comprising predefined plural subsets of the electronic item and corresponding cryptographic hashes (see column 10, line 58 through column 11, line 33) and column 17, lines 5-20); and discloses generate a random challenge (see column 9, lines 25-28); (c) computing a cryptographic hash of a portion of the electronic item corresponding to the selected predefined subset (see column 11, lines 22-51); and (d) testing whether the computed cryptographic hash corresponds to a corresponding cryptographic hash within the presented credential (see column 11 line 55 through column 12, line 31). **Benson** further discloses repeating the step of verifying credential (see claim 51). **Benson** does not explicitly teach randomly selecting one of the predefined plural subsets. However, **Shavit** in an analogous art teaches randomly selecting one of the predefined plural subsets (see column 11 lines 49-57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Benson** to select randomly one of the predefined plural as taught by **Shavit** in order to maintain control over those parties able to use the software (see column 12, lines 56-58). This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Shavit** so as to maintain control over those parties able to use the software.

As per claim 3, Shavit discloses the limitation of further including: randomly selecting a second portion of the electronic item that does not correspond to one of the predefined plural subsets (see column 16, lines 48-54); and requiring computation of a cryptographic hash of said second portion of the electronic item (see column 16, lines 48-54 and see column 12, lines 56-58).

As per claim 4, Benson discloses the limitation of wherein step (c) includes challenging the electronic item to compute said cryptographic hash (see column 13).

As per claim 5, Benson discloses the limitation of wherein step (c) includes accessing the electronic item via shared memory (see column 16, lines 47 et seq.).

As per claim 6, Shavit discloses the limitation of wherein steps (b) and (c) are performed during execution of the electronic item (see column 12, line 53 through column 13, line 4).

As per claims 14, 20, and 21 Benson substantially teaches a method for certifying an electronic item comprising: (a) selecting plural portions of the electronic item (see column 8); (b) computing at least one cryptographic value corresponding to each of the selected plural portions (see column 8) and (c) specifying a credential defining each of the randomly selected plural portions and the corresponding computed cryptographic values (see columns 8 and 13). **Benson** further discloses repeating the step of verifying credential (see claim 51). **Benson** further

discloses generate a random challenge (see column 9, lines 25-28). **Benson** does not explicitly teach randomly selecting plural portions of the electronic item. However, **Shavit** in an analogous art teaches randomly selecting plural portions of the electronic item (see column 11 lines 49-57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Benson** to select randomly one of the predefined plural as taught by **Shavit** in order to maintain control over those parties able to use the software (see column 12, lines 56-58). This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Shavit** so as to maintain control over those parties able to use the software.

Claim 8 recites the limitation of the rejected **claim 1**. Therefore, **claim 8** is rejected on the same rationale as the rejection of **claim 1**.

As per claims 9, 12, 17, and 24, Benson substantially teaches the claimed system of claim 7. **Benson** does not explicitly teach randomly issuing the challenge during execution of the application and selecting a virtual path within the application. However, **Shavit** in an analogous art teaches the limitation of: wherein the challenge generator issues the challenge during execution of the application by the insecure computing arrangement (see column 12, line 53 through column 13, line 4); and wherein the challenge generator selects a virtual path within the application (see column 5, lines 55-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Benson** to select a virtual path and challenge during execution of the application as taught by **Shavit** in

order to maintain control over those parties able to use the software (see column 12, lines 56-58). This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Shavit** so as to maintain control over those parties able to use the software.

As per claims 15 and 22, Benson discloses the limitation of wherein computing step (b) comprises computing a cryptographic hash value corresponding to each of the selected plural portions (see column 13).

As per claims 16 and 23, Benson discloses the limitation of wherein the challenge generator selects a virtual path within the application (see column 9, lines 40-45).

As per claims 18 and 25, Benson discloses the limitation of further including the step of digitally signing the credential (see column 11, lines 42-51).

As per claims 19 and 26, Benson discloses the limitation of further including the step of encrypting the credential (see column 11, lines 23-33).

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin

Patent Examiner

January 9, 2004

Emmanuel L. Moise

EMMANUEL L. MOISE
PRIMARY EXAMINER